REMARKS

The 13 February 2003 official action addressed claims 1-9. Claims 1-3 are amended. New claims 10-15 are added. Claim 1-15 are pending for reconsideration.

1. Overview of amendments

Claim amendments

Independent claims 1, 2 and 3 are amended to clarify their language. In particular, these claims are amended to clarify that a process of updating a cryptosystem key is performed prior to decrypting secret information. If the access is legal, the updated cryptosystem key will correctly decrypt the secret information. If the access is illegal, the updated cryptosystem key will not correctly decrypt the secret information.

New dependent claims 10, 12 and 14 specify that the updating process includes decrypting the secret information correctly, re-encrypting it using a different key, and then updating the cryptosystem key for decrypting the secret information, so that it either will or will not decrypt the secret information correctly, depending on whether the access is legal or illegal.

New dependent claims 11, 13 and 15 specify that the access that triggers the updating process is an attempted illegal access to the secret information. These claims differentiate from the broader recitation of their corresponding independent claims, in which updating may be performed in response to other access events, such as an illegal access to the system itself.

No new matter is added.

2. Response to objections and rejections

Prior art rejections

All claims were rejected under 35 USC §103(a) as being obvious over McDonnal (U.S. 5,699,428) in view of assertions made by the examiner. It is

believed that the claims will be seen to be patentably distinguished from McDonnal in view of the following discussion.

The claimed invention involves protecting secret information that is stored in a computer, such as software or data. In accordance with the claimed invention, the secret information is stored in an encrypted form in a secret information storage, and a cryptosystem key that the system will use to decrypt the secret information is stored in a cryptosystem key storage means. When a user access the system, a cryptosystem key updating procedure is performed. If the access is legal, the updating procedure results in the storage of an updated cryptosystem key that will correctly decrypt the secret information. On the other hand, if the access is illegal, the updating procedure results in the storage of an updated cryptosystem key that will not correctly decrypt the secret information. The updating procedure is performed for each access, prior to decrypting the secret information for the user. Therefore, if the access is illegal, the user will be provided with incorrectly decrypted secret information. In the preferred embodiment, upon each access, the secret information is decrypted correctly, then re-encrypted using a new key, and then the key for decrypting the re-encrypted secret information is updated either correctly or incorrectly, depending on whether the access is legal or illegal.

The features of McDonnal are different than those of the claimed invention. McDonnal also pertains to a system for storing encrypted data. McDonnal's objective is to provide automatic encryption, decryption and re-encryption on an as-needed basis (col. 4, line 66 - col. 5, line 4). McDonnal provides a variety of solutions that help this objective to be reached efficiently. The solutions are summarized in the Summary section of the reference. Briefly, McDonnal provides the following solutions: **1)** using exclusion lists, so that all non-excluded files are automatically decrypted and re-encrypted (col. 5, lines 7-61); **2)** having exclusion lists that pertain to certain types of files (e.g. backup files) for which automatic re-encryption is not necessary (col. 5, line 62 - col. 6, line 9); **3)** performing encryption only upon file open and close commands rather than upon file read and write commands (col. 6, lines 10-45); **4)** delaying re-encryption for files used by certain special applications (col. 6, line 46 - col. 7,

line 5); **5)** delaying retries of failed encryption and re-encryption (col. 7, lines 6-22); **6)** re-encrypting only upon the last close command where multiple applications are using a file simultaneously (col. 7, lines 23 - 49); **7)** including or excluding files for encryption based on their directories (col. 7, line 50 - col. 8, line 5); **8)** choosing different encryption algorithms based on the file type of the file to be encrypted (col. 8, lines 6-49); **9)** making a copy of an encrypted file and decrypting the copy, so that if no changes are made, an encrypted version is already stored and the decrypted copy is simply deleted (col. 8, lines 50-67).

From this summary it is seen that McDonnal's methods are directed to decrypting a file correctly so that a user can access the file, and re-encrypting the file automatically when the user is done with the file so that the file is not inadvertently left in an unencrypted form (see, e.g., col. 11, lines 41-46). In contrast, the claimed invention is directed to cryptosystem key updating in a manner that causes a file to be decrypted ***incorrectly*** when an illegal access occurs so that the user is not able to obtain a correctly decrypted file.

Applicant has reviewed McDonnal in detail, but has found no teaching in McDonnal of the particular features employed by the claimed invention. Figure 2b appears to be the only portion of McDonnal that addresses actions taken when a user is determined to have invalid access rights (226). In that instance, the system forces a "failed open" (228). The corresponding description in the text does not explain what is meant by a failed open, but seems to suggest that if user rights are invalid, a requested file is simply not opened (see col. 19, lines 1-5). In contrast, in accordance with the invention, the determination that an access is illegal has an impact on a cryptosystem key update that is performed ***before*** the file is decrypted and provided to a user. Namely, the detection of an illegal access causes a cryptosystem key to be stored that cannot correctly decrypt the encrypted secret information, such that subsequent decryption of the secret information using that key produces an incorrect result. McDonnal does not teach this type of operation. It is believed that this difference is clearly expressed in the revised claims.

The aforementioned feature is found in each of independent claims 1, 2 and 3 and makes those claims and their dependent claims allowable over the

cited reference. The dependant claims are further allowable for the additional novel features recited therein. For example, claims 10, 12 and 14 specify that the updating process includes decrypting the secret information correctly, re-encrypting it using a different key, and then updating the cryptosystem key for decrypting the secret information, so that it either will or will not decrypt the secret information correctly, depending on whether the access is legal or illegal. This feature is not taught or suggested by McDonnal.

The foregoing amendments and remarks address all bases for objection and rejection and are believed to place the case in condition for allowance. The examiner is invited to contact the undersigned to resolve any remaining issues.

Respectfully submitted,

By David A. Blumenthal

Date: May 12, 2003

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, applicant hereby petitions for such extension under 37 C.F.R. 1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.